



November 15 -17, 2005: Town & Country Convention Center - San Diego, CA

Information Assurance (Certification & Accreditation)

Skip Thaeler


Navy Certification Authority (IA)

COMSPAWARSYSCOM

17 November 2005

What is the DIACAP?

- Defense Information Assurance Certification and Accreditation Process (DoDI 8510.bb)
- New process for certification and accreditation (C&A) of all DoD information systems (IS)
- Replaces DITSCAP; cancels DODI 5200.40 and DoD 8510.1-M

	Department of Defense INSTRUCTION	SDI06 DRAFT Version 6.1 October 1, 2004
		NUMBER 8510.bb ASD (CNI)
<hr/>		
SUBJECT: DoD Information Assurance Certification and Accreditation Process (DIACAP)		
References: (a) Section 3541 of title 44, United States Code, "Federal Information Security Management Act of 2002" (FISMA), (b) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002 (c) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, (hereby canceled) (d) DoD Manual 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July, 2000, (hereby canceled) (e) through (g), see enclosure 1		
1. PURPOSE		
This Instruction:		
1.1. Establishes the standard DoD process for identifying, implementing, and validating IA Controls, for authorizing the operation of DoD information systems, and for managing IA posture across DoD information systems consistent with the Federal Information Security Management Act (FISMA) (reference (a)) and DoD Directive 8500.1 (reference (b)).		
1.2. Supersedes DoDI 5200.40 and DoD 8510.1-M, (references (c) and (d)).		
1.3. Guides DoD information systems in achieving compliance with the information assurance (IA) component of the Global Information Grid (GIG), developed in accordance with DoDD 8100.1 (reference (a)).		
1.4. Supports net-centricity ¹ through an effective and dynamic IA certification and accreditation (C&A) process for providing visibility and control of the implementation of IA capabilities and services and authorizing the operation of DoD information systems, to include core enterprise services and Web Service-enabled software systems and applications.		
2. APPLICABILITY AND SCOPE		
¹ See for example the <i>Department of Defense Net-Centric Data Strategy</i> , prepared by DoD Chief Information Officer (CIO), (May 9, 2003).		
1		

What Are Key Features of the DIACAP?



- Dynamic process
- IA posture reviewed not less than annually
- DoD enterprise C&A decision structure
- DIACAP Intent -- responsibility of DoD Senior Information Assurance Official (SIAO) and Principle Approving Authority (PAA) reps; establishes DIACAP objectives, context & decision structure
- DIACAP Scorecard -- conveys compliance with assigned IA Controls and the IS C&A decision status
- Implements baseline (enterprise) level IA Controls based on the IS Mission Assurance Category (MAC) and Confidentiality Level (CL)
 - IA Controls may be augmented at the DoD Component level and IS level

DITSCAP - DIACAP Overview



DITSCAP

Security requirements and standards uniquely determined by each system

DAA and Certifier selected by/for each system

Policy advocated tailoring, but process was hard-coded to phases

Accreditation status communicated via letter and status code (ATO, IATO) in SSAA

No process improvement

Inaccurate association of ATO with perfect and unchanging security

“Fire and forget” accreditation; 3 year “white glove inspection” reaccreditation

DIACAP

All systems inherit enterprise standards and requirements

Certifier is a qualified, resourced, and permanent member of CIO staff

No pre-defined phases. Each system works to a plan that aligns to the system life cycle

Accreditation status communicated by assigned IA Controls’ compliance ratings and letter and status code (ATO, IATO, IATT, DATO) in DIACAP Scorecard

Automated tools, enterprise managed KS, requirements tied to architecture

ATO means security risk is at an acceptable level to support mission and live data

Continuous, asynchronous monitoring; no reaccreditation; reviewed not less than annually; FISMA reporting

DIACAP Knowledge Service Overview



What is the DIACAP Knowledge Service (KS)?

- A Web-based, DoD PK-enabled DIACAP knowledge resource that provides current GIG IA Certification and Accreditation guidelines
- Developed under sponsorship of ASD(NII) and owned by DoD under the contractual conditions of the IATAC
- A library of tools, diagrams, process maps, documents, etc., to support and aid in execution of the DIACAP
- A collaboration workspace for the DIACAP user community to develop, share and post lessons learned & best practices
- A source for IA news and events and other IA-related information resources

How Can the DIACAP Knowledge Service Support DoD Clients?



- Find the most current GIG IA Certification and Accreditation (C&A) guidelines
- Determine which enterprise level IA Controls apply to a given information system
- Find implementation guidance and validation procedures and expected results for each DoDI 8500.2 IA Control
- Hear about real-world experiences implementing DIACAP
- Get access to forms, templates and collaborative workspace
- Find out about latest IA news

What is eMASS?



- An OASD(NII) Research & Development Initiative owned by DoD under the contractual conditions of the IATAC
- A Web-based suite of integrated services for select core IA program management processes, the first of which is the implementation and management of C&A based on the requirements of the DIACAP
- Designed to support the DoD 8500-series policy framework
- Planned to support DCID 6/3 (Intelligence Community) and NIST SP 800-37/53 (Civil) in future iterations
- Considered a DoD Core Enterprise Services (CES) candidate for IA program management
- An IATAC endeavor – Government owned, not proprietary

What are the benefits of eMASS?



Automation

- Creates a C&A “package” for management of each registered information system

• Accountability

- DoD PKI and auditing features enable tracking of each transaction

• Extensibility

- Scalable to any enterprise, regardless of size and mission

• Flexibility

- Designed to support multiple IA requirements types

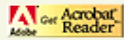
Overview of eMASS

eMASS Reports ~ DIACAP Scorecard

***** SENSITIVE *****

eMASS Enterprise Mission Assurance Support System [Home](#) [View Workload](#) [Help](#) [Edit Profile](#) [Log Out](#)

Certification and Accreditation Module

Returned Digital Score Card [Download PDF Version](#) 

DRRS Defense Readiness Reporting System Organization: OSD System Status: ATO Revalidation Date: 15 Jul 04
System Type: Enclave System Category: Infrastructure System Classification: Confidential

ATO Granted This DoD information system is authorized to conduct full operations at a specified MAC and confidentiality level.
14 Sep 04: by DLA There is no residual risk, or there is an acceptable risk without operational restrictions.

DoDI 8500.2 Subject Area	Control Acronym	DoDI 8500.2 Controls	Compliant/ Noncompliant	Comment	Severity Code (H,M,L)
Security Design and Configuration	DCAR-1	Procedural Review	Compliant		
	DCBP-1	Best Security Practices	Compliant		
	DCCB-2	Control Board	Compliant		
	DCCS-2	Configuration and Specifications	Compliant		
	DCCT-1	Compliance Testing	Compliant		
	DCDS-1	Dedicated IA Services	Compliant		
Identification and Authentication	IAKM-2	Key Management	Compliant		
	IATS-2	Token and Certificate Standards	Compliant		
Enclave and Computing Environment	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting	Compliant		
	ECCD-2	Changes to Data	Compliant		

***** SENSITIVE *****

[Privacy Statement](#) | [Accessibility](#) | [Security Notice](#)

DIACAP Transition



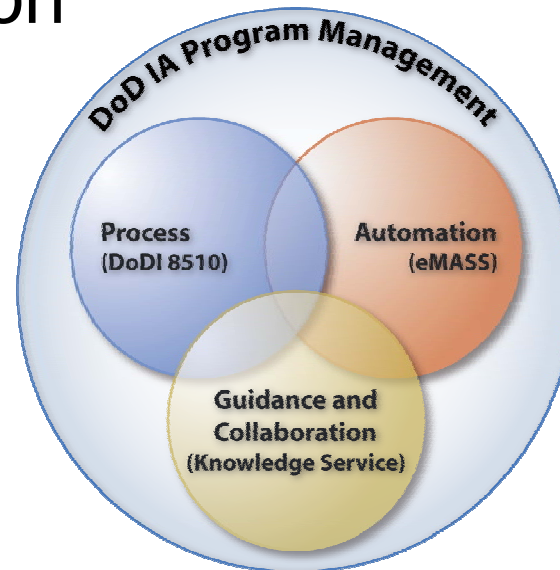
- DoDI 8510.bb (current draft) provides a transition timeline and instructions
- If an unaccredited new start or operational information system (IS), initiate DIACAP
- If currently under DITSCAP, transition actions and timelines vary depending on the DITSCAP phase and status of the SSSA, DITSCAP Accreditation Decision, and incorporation of 8500 IA Controls
- Under specific circumstances, an IS may continue under DITSCAP and be granted an Accreditation Decision under DITSCAP, while required to develop a DIACAP transition plan and schedule
- If an IS has a DITSCAP ATO more than three years old, initiate DIACAP

DIACAP Status



- DIACAP Instruction – DoDI 8510.bb
 - ASD(NII) adjudication of Formal SD-106 comments is near- completion; ASD(NII) to review and sign
 - Estimated issuance: Jan 06
- DIACAP Knowledge Service (KS)
 - Initial increment developed
 - Available upon issuance of DoDI 8510
- eMASS
 - Initial release currently being fielded at select pilot locations

- **DIACAP** – Dynamic C&A Process replacing DITSCAP
- **DIACAP Knowledge Service and eMASS** – DoD-owned Web-based services for DIACAP implementation



Topics for Discussion



- eMass/Knowledge Service Pilot Programs
 - Monterey
 - San Diego
- Fn IA Compliance Certification
- C&A: Single System to FoS Perspective
- White Paper “Product” for IA Session:
 - Points of clear agreement
 - Follow-on actions, issues, objectives

BACKUP

- Access to the Knowledge Service and eMASS requires:
 - DoD PKI certificate (Common Access Card (CAC)), or ECA certificate in conjunction with DoD sponsorship, e.g., for DoD contractors without a CAC/working off-site
 - Future iterations will provide for role-based access
- Availability
 - DIACAP Knowledge Service -- will be available on-line without charge
 - eMASS -- will be available without charge for licensing or development upgrades; organizational investment required for hardware, COTS software licenses and training (further information available upon request)